HELP ?

The growth of economic espionage: America is Target Number One

Foreign Affairs; New York; Jan/Feb 1996; Schweizer, Peter;

Volume: 75
Issue: 1
Start Page: 9
ISSN: 00157120
Subject Terms: Policy making
Manycountries
Industrial espionage
High technology
Competitive intelligence
National security
High tech industries
Espionage
Economic conditions
Classification Codes: **9190**: *US*
9180: *International*
5400: *Research & development*
1120: *Economic policy & planning*
Geographic Names: US

Abstract:
As economic strength becomes the new currency of national power, theft of high-tech secrets is displacing old-fashioned spying. The US must protect its companies, but it should not join in this euphemism for mercantilism.

Full Text:

[Headnote]
America Is Target Number One

Shortly after CIA officer Aldrich "Rick" Ames began selling secrets to the Soviet KGB in 1985, a scientist named Ronald Hoffman also began peddling classified information. Ames, the last known mole of the Cold War, received $4.6 million for names of CIA informants before he was apprehended in early 1994. But Hoffman, a project manager for a company called Science Applications, Inc., made $750,000 selling complex software programs developed under secret contract for the Strategic Defense Initiative (SDI). Hoffman, who was caught in 1992, sold his wares to Japanese multinationals-- Nissan Motor Company, Mitsubishi Electric, Mitsubishi Heavy Industries, and Ishikawajima-Harima Heavy lndustries--that wanted the information for civilian aerospace programs.

Ames received the more dramatic and sensational coverage, as he should have, given that his betrayal led to the loss of life. But the Hoffman case represents the future of intelligence. While one spied for America's chief military rival, the other sold information to a major economic competitor. Perhaps it should induce an epiphany of sorts that these two cases occurred in near congruence.

As economic competition supplants military confrontation in global affairs, spying for high-tech secrets with commercial applications will continue to grow, and military spying will recede into the background. How the United States elects to deal with this troubling issue will not only determine the direction of the American intelligence community, but also set the tone for commercial relations in the

global marketplace.

THE NEW CURRENCY OF POWER

Most economic agents systematically collect **economic intelligence** using legal means. Major corporations collect business intelligence to read industry trends and scout the competition. Many nations track global and regional economic trends and even technological breakthroughs to aid policymakers. But a growing number of states have become very active in gathering intelligence on specific industries or even companies and sharing it with domestic producers. Indeed, economic espionage, the outright theft of private information, has become a popular tool as states try to supplement their companies' competitive advantage. This is sheer folly, threatening to restore mercantilism through the back door.

The United States has devoted in- creasing attention to intelligence on economic issues, sometimes with diplomatic consequences. French Interior Minister Charles Pasqua summoned U.S. Ambassador Pamela Harriman to his office on January 26 of this year to protest U.S. spying on French commercial and technological developments. According to Le Monde, CIA agents flush with 500- franc notes tried to bribe a member of the French parliament to reveal France's negotiating position on the nascent World Trade Organization. A senior official in the Ministry of Communications was offered cash for intelligence on telecommunications and audiovisual policy. A technician for France Telecom, the national telephone network, was also approached. All three immediately notified the French Directorate of Territorial Surveillance, which ordered them to play along with the Americans and lay a trap.

More recently, an October 15 story in The New York Times disclosed that American intelligence agents assisted U.S. trade negotiators by eavesdropping on Japanese officials in the cantankerous dispute over car imports. U.S. Trade Repre- sentative Mickey Kantor and his aides were the reported beneficiaries of daily briefings by the CIA, including information gathered by the CIA'S Tokyo station and the National Security Agency's vast electronic network. How useful this information was remains open to debate. After all, the agreement the United States and Japan ultimately reached was hardly an unambiguous victory for Washington.

These reports, which appear to be accurate, indicate that the United States is following the model for **economic intelligence** several recent CIA directors have proposed. In 1991, believing that the CIA could make a "unique contribution" by uncovering foreign economic espionage in the United States and gathering information about the attempts of other governments to violate international trade agreements and "other basic rules of fair play," Robert Gates called for a deeper look at applying the tools of intelligence to economic matters. By 1993, James Woolsey had declared no more Mr. Nice Guy and promised that the CIA would sniff out unfair trade practices and industrial espionage directed against American firms.

Even with all this heightened activity and interest, the United States is far less involved in economic espionage than most of its major allies and trading partners. Spying on trade negotiators and attempting to obtain commercial information to assist government policymakers is economic espionage at its most benign level and should be expected. The United States has yet to surmount the critical firewall of passing purloined information to domestic companies competing in the global marketplace. It is in this area that the most damage is done to the international trading system and where most major industrialized countries have operated.

Over the past 15 years, the FBI has chronicled numerous cases involving France, Germany, Japan,

Israel, and South Korea. An FBI analysis of 173 nations found that 57 were covertly trying to obtain advanced technologies from U.S. corporations. Altogether, 100 countries spent some public funds to acquire U.S. technology. Former French Intelligence Director Pierre Marion put it succinctly when he told me, "In economics, we are competitors, not allies. America has the most technical information of relevance. It is easily accessible. So naturally your country will receive the most attention from the intelligence services."

Recent data indicate that American industry has felt the effects of such unwanted attention. A 1993 survey commissioned by the American Society for Industrial Security found a dramatic upswing in the theft of proprietary information from corporate America. The number of cases increased 260 percent since 1985; those with foreign involvement shot up fourfold. A 1993 study by R. J. Heffeman and Associates noted that an average of about three incidents every month involve the theft of proprietary information from American companies by foreign entities. These estimates are probably conservative. Companies prefer not to admit they have been victims. An admission can depress the price of their stock, ruin joint ventures, or scuttle U.S. government contracts.

The sort of espionage that threatens U.S. corporations varies with the national characteristics and culture of the perpetrators. France possesses a welldeveloped intelligence service, one of the most aggressive collectors of **economic intelligence** in the world. Using techniques often reminiscent of the KGB or spy novels, the French in recent years have planted moles in U.S. companies such as IBM, Texas Instruments, and Corning. Japan lacks a large formal intelligence service such as the CIA or Direction Generale de la Securite Exterieure (DGSE) but remains an active acquirer of business information. A public-private partnership has evolved between the Ministry for International Trade and Industry and the Japan External Trade Organization, supplementing and nurturing the already well-developed commercial intelligence networks created by Japanese corporations. These commercial networks rival the intelligence services of medium-sized nations. Matsushita's intelligence operations in the United States, for example, occupy two full floors of a Manhattan skyscraper, according to Herb Meyer, special assistant to CIA Director William Casey during the Reagan administration.

THE GAINS FROM THEFT

That so many states practice economic espionage is a testament to how profitable it is believed to be. Marion boasts that during his tenure, France won a $2 billion airplane deal with India thanks to the work of the DGSE. The late French spy chief Count de Marenches typified the French view when he wrote in his memoirs that economic espionage is "very profitable. . . . In any intelligence service worthy of the name you would easily come across cases where the whole year's budget has been paid for in full by a single operation."

Economic espionage threatens to unhinge certain post-Cold War goals such as arms control. On-site inspections, a necessity for some agreements, create institutional opportunities to engage in espionage. The Chemical Manufacturers Association, for example, fears that a chemical weapons treaty with a rigid on-site verification regime could subject 50,000 industrial sites in the United States to systematic international inspection and monitoring. Officials from any number of countries would have access to sensitive information about the American chemical industry, including plant layouts, production levels, perhaps even formulas.

Intelligence collection is a proper function of the state--protecting the national interest and informing statecraft. But collecting proprietary information and sharing it with domestic producers is an entirely different matter. That kind of economic espionage ought to be called what it is: at best a subsidy to

well-connected domestic companies, at worst theft on a par with piracy. Economic espionage can grossly disrupt trade and corrode a nation's science and technology base. It is a parasitic act, relying on others to make costly investments of time and money. And to destroy the rewards of investment is to destroy the incentive to innovate.

THE QUAINT UNITED STATES

This is a decidedly minority point of view in the world marketplace. The rest of the world does not share the American capitalist ethos of vigorous but open competition. In both Europe and Asia, the American law that bars U.S. corporations from bribing foreign officials is viewed as quaint. Antitrust laws are likewise dismissed as an American idiosyncrasy. The semi-corporatist cultures of continental Europe and Asia view the state-business relationship very differently than does the United States. There is a popular old joke in American business circles: "What are the nine scariest words in the English language?" "I'm from the government and here to help you." This quip would hardly garner a smile in Tokyo, Paris, or Berlin.

Early indications are that Russia is more likely to embrace the semi-corporatist view than the American laissez-faire model. The transition from communism to capitalism means only that Russian intelligence will have a greater business orientation. Russian intelligence officials speak of nonbudgetary resources for defense and security policy. And as James Sherr of Oxford University pointed out in the winter 1994-95 National,Interest, Russian intelligence officials are blurring the distinction between, if not merging, state policy and private pursuits. The newly created Federal Agency for Government Communications and Information indicates this trend. Encompassing the former KGB'S communications assets, it is both a "strictly classified organization" and a business, with the right to contract with foreign investors, invest in foreign commercial entities, and set up companies abroad.

As economic strength in part replaces military might as the currency of national power, one can only expect this trend to continue. Trade talks have supplanted arms control as the most acrimonious, demanding, and headline-grabbing form of diplomacy, a certain sign of changing priorities. Consequently, most intelligence organizations around the globe are all too willing to serve as a competitive tool to protect budgets in lean times.

The current interregnum between the Cold War and the new era of economic conflict provides an opportunity finally to address this issue. Fissures or disagreements within the Western alliance no longer have the dangerous consequences they might have had at the height of the Cold War. The United States needs to treat economic espionage not only as an intelligence issue, but as the competitiveness and economic issue it has become. Until it does, the American response will be spotty, and the results minimal.

In 1991 the FBI began a quiet shift from the traditional focus of its counterintelligence policy. The country criteria list, which identified nations whose intelligence services needed watching, has been replaced by the national security threat list, which identifies key American technologies and industries that should be protected. This is an important first step. But even a successful counterintelligence operation will accomplish little unless there are consequences for those who are caught. In the past, ensnared thieves usually received a slap on the wrist. When prosecuted in a court of law, it has usually been under statutes that make it illegal to transfer stolen goods across state lines. This is a difficult legal standard, particularly since some judges believe that information is not a good.

Changes in U.S. law and greater diplomatic fortitude offer the best hope for grappling with this

problem. When Hitachi admitted in court that its employees tried to purchase stolen "Adirondack" computer design workbooks from IBM, the judge in 1983 fined the company a whopping $10,000. The U.S. government did not blink an eye. Several months after the trial, Hitachi reportedly won a major contract to equip the Social Security Administration with computers. (Ironically, the losing bid was submitted by IBM.) When it was disclosed that between the early 1970S and late 1980S the French DGSE had planted agents in Texas Instruments, IBM, and Corning and shared the purloined information with Compagnie des Machines Bull, the U.S. government merely sent a letter of diplomatic protest. Likewise, when Israeli intelligence officers stole valuable technological data from Illinois defense contractor Recon Optical, no penalties were imposed. Selling SDI computer software programs did get Ronald Hoffman a six-year prison term, but the Japanese companies that purchased the data faced no sanctions. This state of affairs should be unsatisfactory.

The United States should consider changing its privacy laws. The data protection laws of countries such as Austria, France, Switzerland, Belgium, Germany, New Zealand, Denmark, Norway, and Luxembourg define "persons" to include corporations for protection of privacy purposes. Their laws provide a much higher level of protection for corporate information, treating business secrets as equivalent to the private data of individual citizens. Under much more firmly defined privacy statutes, thieves could be prosecuted.

When diplomats are involved, the United States should be as aggressive and vigorous as it was when dealing with Soviet spying, or at least as firm as France was last January. Instead, diplomatic personnel have simply been asked to leave quietly, a gesture with little punitive effect. Foreign corporations involved in the theft of American technology or corporate information should face real monetary costs for their crimes. Until there is a price to be paid, companies will not think twice about purchasing and using stolen information, and foreign governments will not blink at stealing American proprietary business information.

How the United States chooses to deal with this problem will set the tone internationally. Some, such as former CIA Director Stansfield Turner, have proposed an American economic espionage program, in effect imitating foreign competitors. But this path is fraught with peril. There is no groundswell of support for such a course in either corporate America or the intelligence community. Ask intelligence professionals what they think about the idea and they are likely to tell you, "I will risk my life for America, but not General Motors." An economic espionage program could also have a corrupting influence on the U.S. intelligence community, as officials might be enticed by bribes from companies seeking particularly useful information. Likewise, American companies are nervous about getting entangled with the intelligence world and the strings that are likely to be attached to any such program. Rather than wanting to imitate its competitors, corporate America seeks a level playing field and protection from industrial thieves.

The goal of the United States should be a world in which governments do not try to outspend one another on stealing each other's corporate secrets. But that goal cannot be reached until the United States decides to grow up and face down the threat. Ignoring economic espionage will not make it go away.

[Author note]

PETER SCHWEIZER is a Visiting Scholar at the Hoover Institution and author of Friendly Spies: How America's Allies Are Using Economic Espionage to Steal Our Secrets.